

REMARKS/ARGUMENTS

Reconsideration and allowance of this application are respectfully requested.

Currently, claims 1-14 and 16-22 are pending in this application.

Rejections Under 35 U.S.C. §103:

Claims 1-4, 8-11, 13 and 15-19 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over Levergood et al (U.S. '780, hereinafter "Levergood") in view of Kirsch (U.S. '915). Applicant respectfully traverses this rejection.

In order to establish a prima facie case of obviousness, all of the claimed limitations must be taught or suggested by the prior art and there must be some suggestion or motivation either in the references themselves or in the knowledge generally available to one of ordinary skill in the art to modify the reference or to combine reference teachings. Applicant respectfully submits that the combination of Levergood and Kirsch fails to teach or suggest all of the claimed limitations. For example, the combination fails to teach or suggest: storing in a resource server authentication details including a unique identifier for a client application of a user and access status data of authorized user, validating the unique identifier, and storing at the resource server (i) the validated identifier for the client application indicating that the client application is associated with a currently authenticated user and (ii) the access status of the user of the client application providing the validated identifier as required by independent claim 1. Independent claim 9 requires similar features.

Accordingly, the present invention relates to validating and storing a unique identifier for a client application (rather than a client terminal). No association of a

unique identifier for a client application (e.g., the web browser) used by a user with authentication data for that user is taught or suggested by the combination of Kirsch and Levergood.

Levergood teaches an internet access control method and monitoring system in which a session identifier (SID) contains an authorization identifier to allow a user to access controlled files (see col. 3, lines 18 to 20). However, in Levergood, the SID is logged in a transaction log by the content server together with the IP address of the user and the SID is validated by the content server using the a digital signature computed *inter alia* from the user IP address (see col. 6, lines 6 to 13). Levergood thus does not provide an authentication scheme suitable for authenticating a user based on uniquely identifying the client application (i.e., the WWW browser) using a unique identifier.

Kirsch discloses performing trans-internet purchase transactions using a persistent predetermined coded identifier (i.e., a “cookie”) established on a client application browser according to an account record stored by the merchant server. In Kirsch, a secure session is established before the existence of an authenticated client server credit relationship is determined. As soon as the secure session is established, any cookie sent to the request URL is also sent to the server.

If a predetermined “credit” relationship exists between the client and the server in Kirsch, then the client-cookie sent to the server enables the cookie to be validated (see col. 7, line 56 to col. 8, line 17). The client-side cookie therefore needs to always contain sufficient information to enable the server to re-authenticate the client (see col. 7, lines 62 to 64). However, the cookie itself in Kirsch is not uniquely identified by the client-server

in such a way that the server is able to confirm that the cookie originates from the user's client application browser. In contrast, the present invention does provide unique information which can be contained in a request to a URL which does uniquely identify the client application as well as associate the user's authentication information with the user's client application.

If no predetermined relationship is pre-recorded on the server in Kirsch, the server provides a form to prompt the client user to provide authentication data which is created and stored as cookie data in a client-side cookie on the client system for use in a subsequent URL purchase request (see col. 8, lines 2 to 4 and 9 to 11). The form itself simply indicates the information required to authenticate the user in future, but does not provide an identifier which can be stored as cookie data as well to identify the user's client application. In Kirsch, the client-side cookie itself therefore does not contain a unique identifier for the client browser for subsequent inclusion in the URL requests and thus there is no way for the server to determine that the client application it has returned the form to is the same client application returning the form-related authentication information. The client-side cookie in Kirsch contains only authentication information provided by the user client.

Accordingly, even if Levergood and Kirsch were combined as proposed by the Office Action, the combination would not have taught or suggested validating and storing a unique identifier for the client application of the user indicating that the client application is associated with a currently authenticated user and the access status of the user of the client application providing the validated identifier as claimed. A record of

the identifier provided is generated by the server and the identifier itself must be validated as well as the user's authentication information which is associated with the validated identifier. When the client application session with the resource server is terminated, the unique identifier is no longer valid. Although the user authentication data need not be affected by the termination of specific session, if a user thus wishes to subsequently reuse the client terminal he/she will need to re-authenticate because a new identifier for the client application will need to be validated and associated with the user's authentication data.

The technique proposed by Kirsch is not as secure as that provided by the present invention as the present invention prevents another user from usurping the user's session by providing a user "identifier" related to the client application as opposed to the client terminal. This name value tag which the server has generated is then used in all subsequent requests sent by the user to identify the user as well as the authentication information which authenticates the user as being allowed access to the system.

Kirsch describes how in subsequent requests to access that web-page or vendor operating the server, a new secure session is established, the client-side cookie is provided to the server, and the authentication data is generated by presenting the confirmation form to the user (see col. 8, lines 53 to 59). However, the server will have no record of the original client application to which the form was provided, only of the authentication data the user originally returned in a cookie. In Kirsch, the client-side cookie specifically encodes sufficient information to authenticate the client user to the terminal, thereby obviating the need for the client user to re-authenticate manually (col. 8,

lines 59 to 63) which enables subsequent transactions to proceed on a one-click basis (see col. 8, line 64 to col. 9, line 3). However, this client-side cookie data relates to user information such as the user's billing address to facilitate the establishment of a client/vendor credit relationship. The data does not associate the user with a particular client application.

Accordingly, Applicant respectfully requests that the rejection of claims 1-4, 8-11, 13 and 15-19 over Levergood and Kirsch be withdrawn.

Claims 5-7, 12 and 14 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over Levergood in view of Kirsch and further in view of See et al.

Applicant respectfully traverses this rejection. Since claims 5-7 depend at least indirectly from independent claim 1 and claims 12 and 14 depend at least indirectly by independent claim 9, Applicant submits that the above comments with respect to the combination of Levergood and Kirsch apply equally to these claims. Applicant submits that See et al fails to remedy the above discussed deficiencies of Levergood and Kirsch. Applicant thus respectfully requests that the rejection of claims 5-7, 12 and 14 under 35 U.S.C. §103 be withdrawn.

New Claims:

New claims 20-22 have been added to provide additional protection for the invention. New claims 20 and 21 require, *inter alia*, "the resource server generating a unique identifier for the client application which enables the user to be uniquely identified in subsequent requests sent by the client application to the resource server." Applicant thus submits that claims 20-21 are allowable. New claim 22 depends from

LEVERIDGE et al.

Application No. 09/446,583

November 3, 2003

claim 1 and is thus allowable for at least the reasons discussed above with respect to claim 1.

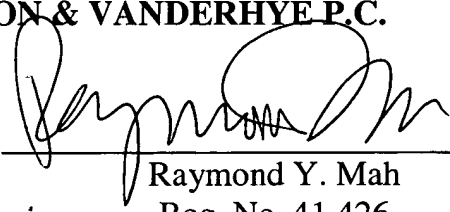
Conclusion:

Applicant believes that this entire application is in condition for allowance and respectfully requests a notice to this effect. If the Examiner has any questions or believes that an interview would further prosecution of this application, the Examiner is invited to telephone the undersigned.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____



Raymond Y. Mah
Reg. No. 41,426

RYM:sl
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4044
Facsimile: (703) 816-4100